UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/316,804	05/21/1999	JOHN RAITHEL HIND	CR9-99-045	8334

25259 7590 07/30/2003

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2131	4

DATE MAILED: 07/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/316,804	HIND ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-18 are pending for examination.

2. Claims 1-18 are rejected.

Specification

3. The disclosure is objected to because of the following informalities: The attempt to incorporate subject matter into this application by reference to US patent applications only by a title (i.e., page 1, lines 9-11, "Method and Apparatus for Efficiently Initializing Secure Communications Among Wireless Devices", and other locations) is improper because reference to said documents is incomplete without more specific identification (i.e., actual US patent applications numbers).

Claim Objections

4. Claims 1, 7, 13 are objected to because of the following informalities: "a server" is recited as "a a server". Appropriate correction is required.

Claims 5, 11, 17 are objected to because of the following informalities: "transmitting said device " is recited as "transmitting said said device ". Appropriate correction is required.

Claim 6 is objected to because of the following informalities: "as claimed in claim 5" is recited as "as claimed in claim 6". The examiner assumes that for the purpose of applying art that the applicant is referring to "claim 5". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 13-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims either recite non-statutory subject matter as they either recite a computer comprising instructions or are disclosed as software alone. Claims including a computer readable medium avoid a rejection under this code, and for the purpose of applying art such a computer readable medium embodiment is assumed.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 13-18 recites the limitation "embedded radio module, said *method* comprising: " in claims 13- 18. There is insufficient antecedent basis for this limitation in the claim in that the preamble recites "A program for initializing...". Claims 13- 18 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1- 3, 5- 9, 11-15, 17- 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Debry, U.S. Patent 6,314,521 B1.

8. As per claim 1 ; " A method for *initializing* [see Debry, col. 6, lines 4-7] a first device distributed with an embedded radio module using a server, said server having an *embedded radio* [col. 6, lines 16-17, col. 7, lines 20-24] module, said method comprising the steps of: sending an *inquiry* [col. 6, lines 33-35, the inquiry as part of the establishment of the HTTP session (i.e., SSL mutual authentication handshaking)], where from said server to said first device using said embedded radio modules; *returning* [col. 6, lines 36-43], from said first device, a *unique device identifier* [col. 6, lines 19-27,40-41, col. 8, lines 17-25] of said first device, to said server; creating, at said server, a *public key, private key pair* [col. 6, lines 56-60] for said first device; creating, at said server, a *device certificate* [col. 6, lines 12-18, col. 9, lines 15-23] for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; *transmitting* [col. 6, lines 52-64] said private key, and said *device certificate* [col. 7, lines 25-26], and a public key of a *Certificate Authority* [col. 6, lines 10-11, col. 8, lines 26-28, 38-44] which signed said device certificate, to said first device; and, storing said private key in *non-removable protected storage* [col. 6, lines 28-32, 66-67] at said first device." ;

And further as per claim 7 ; "A system [This claim is the apparatus of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an

embedded radio module, said system comprising: a communications mechanism for sending an inquiry from said server to said first device using said embedded radio modules, and returning, from said first device, a unique device identifier of said first device, to said server; a processor at said server for creating a public key, private key pair for said first device; a device certificate, created at said server, for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; wherein said communications mechanism transmits said private key, and said device certificate, and a public key of a Certificate Authority which signed said device certificate, to said first device; and, said processor stores said private key in non-removable protected storage at said first device.";

And further as per claim 13 ; "A program [This claim is the software embodiment of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an embedded radio module, said method comprising: computer program code means of sending an inquiry from said server to said first device using said embedded radio modules; computer program code means of returning, from said first device, a unique device identifier of said first device, to said server; computer program code means of creating, at said server, a public key, private key pair for said first device; computer program code means of creating, at said server, a device certificate for said first device, said device certificate having a unique hardware identifier associated with said first device and a public key associated with said first device; computer program code means of transmitting said private key, and said device certificate, and a public key of a Certificate Authority which signed said device certificate, to

said first device; and, computer program code means of storing said private key in non-removable protected storage at said first device. " ;

9. As per claim 5 ; "A method for *initializing* [see Debry, col. 6, lines 4-7] a first device distributed with an *embedded radio* [col. 6, lines 16-17, col. 7, lines 20-24] module using a server, said server having an embedded radio module, said method comprising the steps of: sending an *inquiry* [col. 6, lines 33-35, the inquiry as part of the establishment of the HTTP session (i.e., SSL mutual authentication handshaking)] from said server to said first device using said embedded radio modules; *creating* [col. 6, lines 19-27,40-41, col. 8, lines 17-25], at said first device, a public key, private key pair for said first device; *storing* [col. 6, lines 28-32, 66-67], at said first device, said private key in non-removable protected storage; *returning* [col. 6, lines 36-43], from said first device, a unique device identifier and said public key of said first device, to said server; creating, at said server, a *device certificate* [col. 6, lines 12-18, col. 9, lines 15-23]for said first device, said device certificate having said device identifier and said public key; and *transmitting* [col. 6, lines 52-64] said device certificate and a public key of a *Certificate Authority* [col. 6, lines 10-11, col. 8, lines 26-28, 38-44] which signed said device certificate to said first device." [col. 10, lines 1-60, figure 11, '...the other configuration data determines which request headers will be passed to the Transaction Gateway Client. Some options include *authentication data*, URI, document root, and Web Browser IP address ... '];

And further as per claim 11 ; "An initialization system [This claim is the apparatus of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above], said system comprising: a first device, said first device having an embedded radio module; a server, said server having an embedded radio module; a communications mechanism, said

communications mechanism sending an inquiry from said server to said first device using said embedded radio modules; wherein said first device creates a public key, private key pair for said first device, stores said private key in non-removable protected storage, and returns a unique device identifier and said public key of said first device, to said server; said server creates a device certificate for said first device, said device certificate having said device identifier and said public key; and transmits said device certificate and a public key of a Certificate Authority which signed said device certificate to said first device.";

And further as per claim 17 ; "A program [This claim is the software embodiment of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for initializing a first device distributed with an embedded radio module using a server, said server having an embedded radio module, said method comprising: computer program code means of sending an inquiry from said server to said first device using said embedded radio modules; computer program code means of creating, at said first device, a public key, private key pair for said first device; computer program code means of storing, at said first device, said private key in non-removable protected storage; computer program code means of returning, from said first device, a unique device identifier and said public key of said first device, to said server; computer program code means of creating, at said server, a device certificate for said first device, said device certificate having said device identifier and said public key; and transmitting said device certificate and a public key of a Certificate Authority which signed said device certificate to said first device.";

10. Claim 2 ***additionally recites*** the limitations that "method as claimed in claim 1 wherein said protected storage is *write-only storage* able to perform computations involving previously

written data. ". The teachings of Debry (col. 6, lines 66-67) suggest such limitations (i.e., non-volatile memory);

And further, claim 8 ***additionally recites*** the limitations that "A system as claimed in claim 7 wherein said protected storage is write-only storage able to perform computations involving previously written data. " [This claim is the apparatus of the method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above] ;

And further, claim 14 ***additionally recites*** the limitations that "A program as claimed in claim 13 wherein said protected storage is write-only storage able to perform computations involving previously written data. " [This claim is the software embodiment of the method claim 2, and is rejected for the same reasons provided for the claim 2 rejection above];

11. Claim 3 ***additionally recites*** the limitations that "A method as claimed in claim 1 wherein a copy of said certificate is stored in an *enterprise database.*". The teachings of Debry (col. 6, lines 24-26, 61-64) suggest such limitations (i.e., IBM Corp. wide database is clearly an enterprise database);

And further, claim 9 ***additionally recites*** the limitations that "A system as claimed in claim 7 wherein a copy of said certificate is stored in an enterprise database. " [This claim is the apparatus of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above];

And further, claim 15 ***additionally recites*** the limitations that "A program as claimed in claim 13 wherein a copy of said certificate is stored in an enterprise database. " [This claim is the software embodiment of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above];

12. Claim 6 ***additionally recites*** the limitations that "A method as claimed in claim 5 wherein said protected storage is a write-only storage able to perform computations involving previously written data." . The teachings of Debry (col. 6, lines 66-67) suggest such limitations (i.e., non-volatile memory);

And further, claim 12 ***additionally recites*** the limitations that "A system as claimed in claim 11 wherein said protected storage is a write-only storage able to perform computations involving previously written data." [This claim is the apparatus of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above];

And further, claim 18 ***additionally recites*** the limitations that "A program as claimed in claim 17 wherein said protected storage is a write-only storage able to perform computations involving previously written data." [This claim is the software embodiment of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above];

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 10, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Debry, U.S. Patent 6,314,521 B1, and further in view of Netscape ("Netscape") Communications Corp., "Netscape Certificate Server FAQ", 1997.

13. As per claim 4 ; "A method as claimed in claim 1 wherein a copy of said certificate is stored in an LDAP directory." .

Debry teaches of the certificate based initialization / authentication of a first device associated with a network server / certificate authority in an enterprise (i.e., IBM) environment.

Debry fails to teach of the certificate storage being in an LDAP directory.

Netscape teaches of using the Netscape Certificate Server v1.0 for managing (clearly including storage) PKI based digital certificates in an enterprise-wide security infrastructure scaled to the internet, using open standards including LDAP directory support (2nd section, 1st and 3rd bullets).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Debry certificate based initialization / authentication of a first device associated with a network server / certificate authority in an enterprise environment invention with the Netscape Certificate Server v1.0 for managing PKI based digital certificates in an enterprise-wide security infrastructure, using LDAP directory support to allow for the Open Standards support for PKI based security (i.e., SSL, X.509 directory services, etc.) that is required in such large networks such as the internet (Netscape, entire document).

And further, claim 10 ***additionally recites*** the limitations that "A system as claimed in claim 7 wherein a copy of said certificate is stored in an LDAP directory." [This claim is the apparatus of the method claim 4, and is rejected for the same reasons provided for the claim 4 rejection above];

And further, claim 16 ***additionally recites*** the limitations that "A program as claimed in claim 13 wherein a copy of said certificate is stored in an LDAP directory." [This claim is the software embodiment of the method claim 4, and is rejected for the same reasons provided for the claim 4 rejection above];

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Traw et al U.S. Patent 5,949,877

2. Traw et al U.S. Patent 6,542,610

3. Weber et al U.S. Patent 6,178,409

4. Ramasubramani et al. U.S. Patent 6,233,577

15. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

After-final	(703) 746-7238
Official	(703) 746-7239
Non-Official/Draft	(703) 746-7246

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100